Infoblox

The Infoblox Q3 2020

Cyberthreat Intelligence Report

Disclaimer

Infoblox publications and research are made available solely for general information purposes. The information contained in this publication is provided on an "as is" basis. Infoblox accepts no liability for the use of this data. Any additional developments or research since the date of publication will not be reflected in this report.

Table of Contents

Executive Summary...4

Cybertrends and Challenges..5

The Cybercrime Explosion Continues into 2020...5

Teleworking Creates New Opportunities for Threat Actors......................5

Email and Social Engineering: Prominent Attacker Techniques of Choice 6

Q3 2020 Threat Report Summaries 7

July 2020 Threat Reports and Threat Alerts..........................10

August 2020 Threat Reports and Threat Alerts 18

September 2020 Threat Reports and Threat Alerts 34

Infoblox Cyber Intelligence Unit 48

Infoblox Threat Intelligence.. 48

Executive Summary

Infoblox is pleased to publish our first Infoblox Quarterly Cyberthreat Intelligence Report. We will be publishing these reports during the first month of each calendar quarter. This Q3 2020 report includes our data on threat activity publicly released from July 1, 2020, through September 30, 2020.

This data provides our original research context and insight into significant threats recently observed, detailed analysis of advanced malware campaigns and analysis of recent significant attacks. In some cases, we report and expand on original research published by other security firms, industry experts and university researchers. We feel that timely information on cyberthreats is vital to protect the user community at large.

Infoblox threat reports generally include research on specific threats and related data, customer impacts, analysis of campaign execution, details of attack chains, and vulnerabilities and mitigation steps. We may also share background information on the threat actors likely responsible for the particular incidents under review.

Subscribers to our threat intelligence products and services will receive the full reports, which provide more comprehensive data, including an in-depth list of the indicators of compromise (IOCs) for the specific campaign, as well as other timely alerts and information.

Cybertrends and Challenges

The Cybercrime Explosion Continues into 2020

The 2019 Internet Crime Report[1] published by the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) notes, "This year's Internet Crime Report highlights the IC3's efforts to monitor trending scams such as Business Email Compromise (BEC), Ransomware, Elder Fraud, and Tech Support Fraud. As the report indicates, in 2019, IC3 received a total of 467,361 complaints with reported losses exceeding $3.5 billion. The most prevalent crime types reported were Phishing/Vishing/Smishing/Pharming, Non-Payment/Non-Delivery, Extortion, and Personal Data Breach. The top three crime types with the highest reported losses were BEC, Confidence/Romance Fraud and Spoofing. More details on each of these scams can be found in this report."

We see evidence that these trends will continue to increase over time due to expanding opportunities for exploitation by cyberattackers, such as the recent increase in teleworking. Our researchers continue to see a large emphasis on email campaigns and socially engineered attacks designed to engage victims. In many of the threats we uncover, perhaps a majority, the intended victim must interact and cooperate for the attack to succeed, generating a need for the attackers to create campaigns that will successfully deceive victims.

Teleworking Creates New Opportunities for Threat Actors

Commercial and government enterprises are facing new challenges due to the Coronavirus pandemic. Teleworking has presented vulnerabilities that are more easily exploited by threat actors who continue to move aggressively to leverage these new opportunities.

Remote workers require access to enterprise resources from a variety of endpoints, including both employer-provided and personal laptops, as well as a broad mix of mobile devices. However, many cybersecurity procedures and security controls used within enterprise facilities are unable to provide the same level of security for remote locations. The enterprise security stack is far too complex to work remotely without significant changes, preparation and planning.

The rate at which the pandemic has unfolded has been fast, widespread and unexpected. Organizations have had very little time to alter their existing cybersecurity measures to support a large-scale remote workforce. Consumer Wi-Fi connections, document shares on cloud folders, and home browsers configured with plug-ins and applications are just some of the many vulnerabilities that may introduce substantial risks that were not present before the pandemic.

[1] https://pdf.ic3.gov/2019_IC3Report.pdf

Home routers are not always secure or updated to the level their manufacturers suggest. Workers at home may also be more inclined to view personal emails and other nonbusiness websites on employer-issued devices. Such viewings only increase the probability of encountering malware-laden advertisements (malvertisements) that could potentially compromise workers' devices and, eventually, the enterprise.

Further, attackers are leveraging the widespread demand for information about the severity of the pandemic to lure victims in. Remote workers may easily fall victim to malware-laden links in online forums, social media and small publications whose websites have been compromised. These challenges will remain a constant threat, especially to remote users.

Email and Social Engineering: Prominent Attacker Techniques of Choice

Email campaigns remain one of the top attack vectors for threat actors. According to the FBI IC3, "Business email compromise/email account compromise comprise a scam worth $26 billion dollars."[2] Additionally they say, "Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests. The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds. The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information or Wage and Tax Statement (W-2) forms."

Where these attacks succeed, funds are typically distributed to banks that appear to be located in China or Hong Kong. The FBI has noted that fraudulent transfers are also sent to Mexico, Turkey and the United Kingdom. BEC/EAC constitute just one portion of the large volume of targeted threats using email.

Emails with malicious attachments or URLs directing users to malware-laden websites remain a top threat for commercial, government and home users. Per the Symantec Internet Security Threat Report, the average user will receive 16 malicious spam emails in any given month.[3] Email spam campaigns are a prevalent theme in the research we produce on current threats, and our view is consistent with the FBI's in that email-based scams will continue to grow and evolve through 2020 and beyond.

[2] https://www.ic3.gov/media/2019/190910.aspx

[3] https://docs.broadcom.com/doc/istr-23-2018-en

Q3 2020
Threat Report Summaries

BLM-Themed Malspam Delivers Trickbot Banking Trojan

On June 25, we observed a campaign that used the Black Lives Matter (BLM) movement and the Trickbot malware to lure unsuspecting victims into opening a malicious email and attachment. According to the ThreatPost blog, the attachment, when opened, “surfaces a button urging recipients to ‘Enable Editing’ or ‘Enable Content.’” If clicked, the button activates malicious macros that in turn download TrickBot, in the form of a malicious library (DLL file). This attack is part of a trend that has grown throughout 2020. Previously, we reported on a Trickbot campaign that spoofed an alert from the World Health Organization regarding the coronavirus pandemic. That event is part of the barrage of phishing email campaigns linked to other topics related to COVID-19 and more.

Valak InfoStealer Delivers IcedID Banking Trojan

Between June 24 and July 1, security researcher Brad Duncan reported four malware campaigns that used the Valak malware loader to deliver the IcedID banking trojan. IcedID is designed to steal banking credentials, credit cards and other financial information. Valak is sophisticated modular malware that acts as both a malware loader and an information stealer (infostealer). First observed in late 2019, it quickly evolved, with the creators producing over 30 new versions of the malware in just six months. Valak’s modular nature allows the attackers to rapidly develop and deploy new malicious code to infected systems to expand the malware’s capabilities.

Vidar InfoStealer

From June 25 to 30, we observed a malicious spam (malspam) email campaign distributing the Vidar infostealer, a variant of the Arkei infostealer. Vidar is a trojan infostealer first observed in December 2018. Vidar can steal credit cards, usernames, passwords and files, as well as take screenshots of a user’s desktop. Vidar can also steal wallets for cryptocurrencies such as Bitcoin and Ethereum.

The Return of Emotet

On July 17, Proofpoint’s threat research team observed a malspam campaign delivering the Emotet banking trojan after a five-month hiatus by the threat actor. Emotet steals stored passwords, sensitive banking data and browser histories from victims’ computers. This sizable campaign included nearly a quarter-million malspam messages.

Qakbot Infostealer

On August 3, security researcher Brad Duncan reported a malspam campaign that used compressed Visual Basic Script (VBScript) files to deliver the Qakbot infostealer. Qakbot, also known as Qbot, can steal a victim’s credentials, banking information and files. Qakbot includes worm capabilities that allow it to spread itself to other systems on the same network, as well as rootkit capabilities that help hide its presence and establish persistence on infected clients.

MassLogger Infostealer Malspam Campaign

On August 11, we observed malspam email campaigns distributing MassLogger malware. MassLogger is a relatively new infostealer that was reportedly first observed in April 2020. It is written using .NET, a programming framework developed by Microsoft. MassLogger can log keystrokes and clipboard data, take screenshots and steal credentials from Chrome, Firefox, Outlook, Thunderbird, Discord, NordVPN, FileZilla, Telegram and more.

njRAT Malspam Campaign

On August 24, a malspam email campaign distributed the njRAT malware, also known as Bladabindi and Njw0rm. njRAT is a remote access trojan (RAT) and infostealer first observed in January 2013. njRAT can maintain persistence and operate undetected on victims' machines while transmitting sensitive information back to its command and control (C&C) infrastructure over a period of days or even weeks. In a campaign we reported on in May 2019, njRAT also delivered the Agent Tesla keylogger as part of its attack chain.

Metamorfo Banking Trojan

On August 18, cybersecurity researchers at Menlo Security reported an ongoing malware campaign that used HTML smuggling techniques to deliver the Metamorfo banking trojan. Metamorfo is a banking trojan that attempts to steal sensitive financial information and exfiltrate it to a C&C server. What sets Metamorfo apart from other banking trojans is the wide variety of evasive techniques it uses to bypass security mechanisms and deliver its payload without being detected.

Cyberthreat Advisory—HIDDEN COBRA: BLINDINGCAN RAT Variants

On August 19, the Department of Homeland Security (DHS), the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) released a Malware Analysis Report on malware variants, dubbed BLINDINGCAN, used by the North Korean government. Malicious cyberactivities associated with the North Korean government are commonly referred to as HIDDEN COBRA. BLINDINGCAN refers to a series of RAT variants currently used by HIDDEN COBRA actors to maintain persistent access inside a victim's infrastructure. The target set for this campaign includes government contractors who deal with key military and energy technologies. The threat actors used active job postings from contractors of interest as lures to deliver one of the malware variants to the victim.

Cyberthreat Advisory—HIDDEN COBRA: BeagleBoyz and FASTCash 2.0

On August 26, the CISA published a joint advisory based on analytic efforts with the Department of the Treasury, the FBI, U.S. Cyber Command (USCYBERCOM) and government partners. The report describes tools and techniques used by an element of the North Korean government to carry out attacks against automated teller machines, efforts the U.S. government refers to as "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks." The United Nations considers the BeagleBoyz's activity a means to circumvent UN resolutions and generate funds to support prohibited nuclear weapons and ballistic missile programs. The BeagleBoyz group is part of North Korea's Reconnaissance General Bureau and has been carrying out FASTCash campaigns against banks' retail payment infrastructure since 2016.

Raccoon InfoStealer Malspam Campaign

On September 1, we observed malspam email campaigns distributing Raccoon malware. Raccoon, also known as Racealer, is an infostealer first observed in April 2019. Raccoon can steal credit cards, usernames, passwords and cryptocurrency wallets. Although it has relatively basic features, it is effective and affordable. Threat actors can reportedly purchase Raccoon from online forums for $75, a reportedly lower-than-average price for similar types of malware. Raccoon is a malware as a service (MaaS) that allows buyers to receive software updates and support from the sellers.

Cyberthreat Advisory—APT39 Malicious Activity and Tools

On September 17, the FBI published a new FLASH alert in coordination with the DHS and the Treasury Department. The report describes multiple types of malware that the Iranian Rana Intelligence Computing Company—also known as APT39—has used in its global operations. In the report, the FBI included descriptions of how the various types of malware operate, as well as a set of YARA rules for each type. The FBI also published a representative set of malware samples to VirusTotal for public analysis. Rana Intelligence Computing is a front company for Iran's Ministry of Intelligence and Security (MOIS). According to the FBI, Rana has targeted hundreds of individuals and entities in more than 30 countries spread across Asia, Africa, Europe and North America. It has previously targeted foreign citizens, foreign governments, and organizations predominantly in the travel, hospitality, academic and telecommunications industries. In Iran, Rana has targeted individuals and dissidents, in addition to companies and academic institutions.

WeTransfer—Malicious Spam Campaign Delivers Static Phishing Page

On September 20, Infoblox observed a malspam campaign delivering a malicious HTML file capable of phishing for credentials. While threat actors used generic lures in emails, the HTML file specifically targeted WeTransfer, a file-sharing service. Threat actors used a malicious HTML file in this campaign that is not related to any malware family that we know of. The file harvests and exfiltrates WeTransfer credentials.

Glupteba Backdoor Trojan

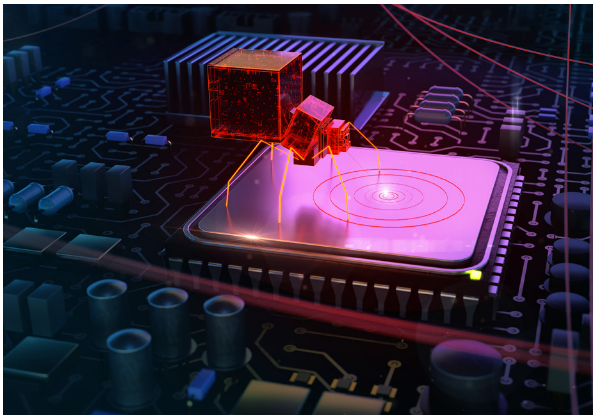
From September 20 to 26, Infoblox detected communications between malicious Glupteba bots and C&C servers in customer DNS traffic. This activity was identified by our Threat Insight security solution, which employs machine learning models to detect and block certain types of malicious behavior, in this case data exfiltration.

July 2020

Threat Reports & Cyberthreat Alerts

BLM-Themed Malspam Delivers Trickbot Banking Trojan

Author: Eric Patterson



Overview

On June 25, Infoblox observed a Black Lives Matters (BLM)-themed malspam campaign delivering Trickbot malware.[1,2,3] The previous Trickbot campaign we wrote about employed an email lure that spoofed an alert from the World Health Organization regarding the Coronavirus pandemic.[4]

Customer Impact

Considered a successor to the Dyre banking trojan, Trickbot was first discovered in 2016 and has since grown in popularity.[5,6,7] Trickbot infects victims, steals sensitive financial information and exfiltrates it to its C&C server. It can also move laterally within a network by brute-forcing Remote Desktop Protocol (RDP) credentials.

Threat actors favor Trickbot due to its modular nature, which facilitates customization and provides attackers the capability to drop additional malware such as Emotet on an infected system.

Campaign Analysis

The emails we observed in this campaign all portrayed themselves to be from official-sounding sources such as the “State Authority” or “Country Administration,” which do not actually exist.

The email subject lines varied, asking the recipient to vote on or express how they felt about the BLM movement. The message bodies followed this theme, asking recipients to anonymously leave their reviews on the subject matter. The bodies also indicated that some sort of claim was attached. The accompanying files were Microsoft Word documents that followed the naming scheme: *e-vote_form <4-5 digits>.doc*.

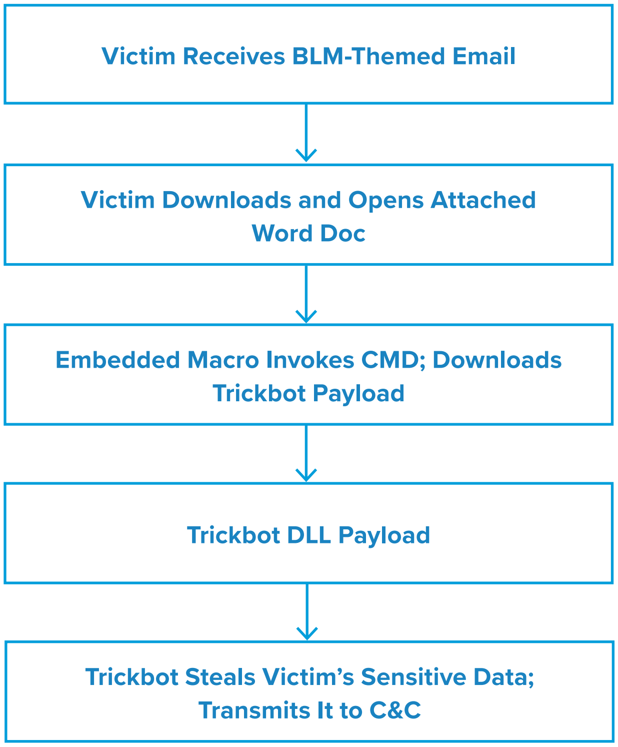
Attack Chain

When the user opens the attached file, they are prompted to “enable editing” and then “enable content.” Once this is done, an embedded macro will invoke *cmd.exe* to download the Trickbot DLL payload.

After Trickbot successfully installs itself, it attempts to steal sensitive victim data, establish communications with its C&C infrastructure to transmit information, and potentially download additional malware onto the infected device.

Some researchers have noted an unexplained delay of up to two weeks from when they enabled content to when they received the Trickbot DLL on their system.

There were no indications that the Trickbot sample in this campaign went on to download additional malware or that it carried out further exploitation. Given the length of time taken to download the TrickBot payload, this may change in the coming weeks if the threat actor(s) have intentionally time-delayed additional malware payloads.



Victim Receives BLM-Themed Email

Victim Downloads and Opens Attached Word Doc

Embedded Macro Invokes CMD; Downloads Trickbot Payload

Trickbot DLL Payload

Trickbot Steals Victim's Sensitive Data; Transmits It to C&C

Vulnerabilities & Mitigation

Trickbot is a prolific banking trojan that is capable of stealing user credentials, invoking additional software such as the Mimikatz password-stealing tool, and gaining machine persistence. Infoblox recommends the following methods for detecting, preventing, and mitigating Trickbot threats:

- Install and run advanced antivirus software that can detect, quarantine and remove malware.
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Develop traffic rules that can block outbound access to potentially malicious endpoints based on domains or unique URI parameters.
- Implement command prompt logging to detect any anomalous or malicious use.
- Install strong email security solutions to detect emails with suspicious content.

Endnotes

1. https://twitter.com/malware_traffic/status/1276193322999123972
2. https://twitter.com/abuse_ch/status/1275526243404972034
3. https://news.zepko.com/black-lives-matter-email-campaign-delivers-trickbot-malware/
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--66
5. https://blog.malwarebytes.com/detections/trojan-trickbot/
6. https://www.fidelissecurity.com/threatgeek/archive/trickbot-we-missed-you-dyre/
7. https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/

Valak Downloader/InfoStealer Delivers IcedID Banking Trojan

Author: James Barnett

Overview

Between June 24 and July 1, security researcher Brad Duncan reported four malware campaigns that used the Valak malware loader to deliver the IcedID banking trojan.[1,2,3,4]

Customer Impact

Valak is a sophisticated modular malware that acts as both a malware loader and infostealer. It was first observed in late 2019 and quickly evolved, with the creators producing over 30 new versions of the malware in the span of just six months.[5] Valak's modular nature allows the authors to rapidly develop and deploy new malicious code to infected systems in order to expand the malware's capabilities.

IcedID is a banking trojan that uses web injection and redirection attacks to steal banking credentials, credit cards, and other financial information from victims who believe they are entering their information into a secure website.

Campaign Analysis

The reports of these Valak campaigns did not specify how the malware was initially distributed, but based on recent reports about Valak's behavior,[6] it is likely that the reported campaigns used a technique known as a "reply chain attack" to deliver the malware via email.

Unlike malspam techniques that use arbitrary email accounts to indiscriminately deliver malicious emails to a large number of targets, reply chain attacks use hijacked email accounts to send targeted replies to legitimate emails sent to the hijacked account. This makes the malicious emails much harder to detect, because they appear to be legitimate responses to existing conversations sent by accounts the recipient already knows.

The bodies of emails in reply chain attacks are generally similar to those of typical malspam messages: they entice the recipients to open an attached file, or download and open a file from a provided link. According to recent reports, Valak has used both file attachments and download links in its reply chain attacks.

Attack Chain

The Valak attack chain begins when the victim downloads a password-protected ZIP file from an email attachment or link[7] and extracts it using a password contained in the body of the email. The extracted file is a malicious Microsoft Word document that instructs the victim to enable macros in order to view its contents.

When the victim does so, the macros within the document contact a PHP-based download proxy to retrieve the initial Valak DLL payload. This behavior is similar to certain versions of Ursnif (a.k.a. Gozi) and some security solutions may incorrectly identify it as such. After downloading the Valak DLL payload, the macros use the Windows Register Server (regsrv32.exe) to register and execute it.

Upon execution, the Valak DLL drops a malicious JavaScript file with an arbitrary name and executes it using the Windows Script Host (wscript.exe). This creates registry keys to store configuration data for Valak's other components. It then reaches out to embedded C&C URLs to download two files. The first is an additional JavaScript payload that Valak saves as text within one of the aforementioned registry keys. The second is an executable that Valak's code refers to as PluginHost.exe, though the name it uses when saving the file varies between campaigns.

After downloading these additional files, the initial Valak JavaScript creates a third JavaScript file that it stores within an Alternative Data Stream (ADS) in an arbitrary file that varies between campaigns. It executes the second JavaScript payload stored in the Windows Registry. The initial JavaScript then creates a scheduled task to execute the third JavaScript, thus establishing persistence on the infected machine.

When Valak's scheduled task launches the second stage JavaScript payload, it executes PluginHost.exe to manage Valak's various plugin modules. It then downloads additional payload(s) from its C&C, saves them as ADSs in arbitrary files, then executes them. In these campaigns, the payload it delivered was an installer for the IcedID banking trojan.

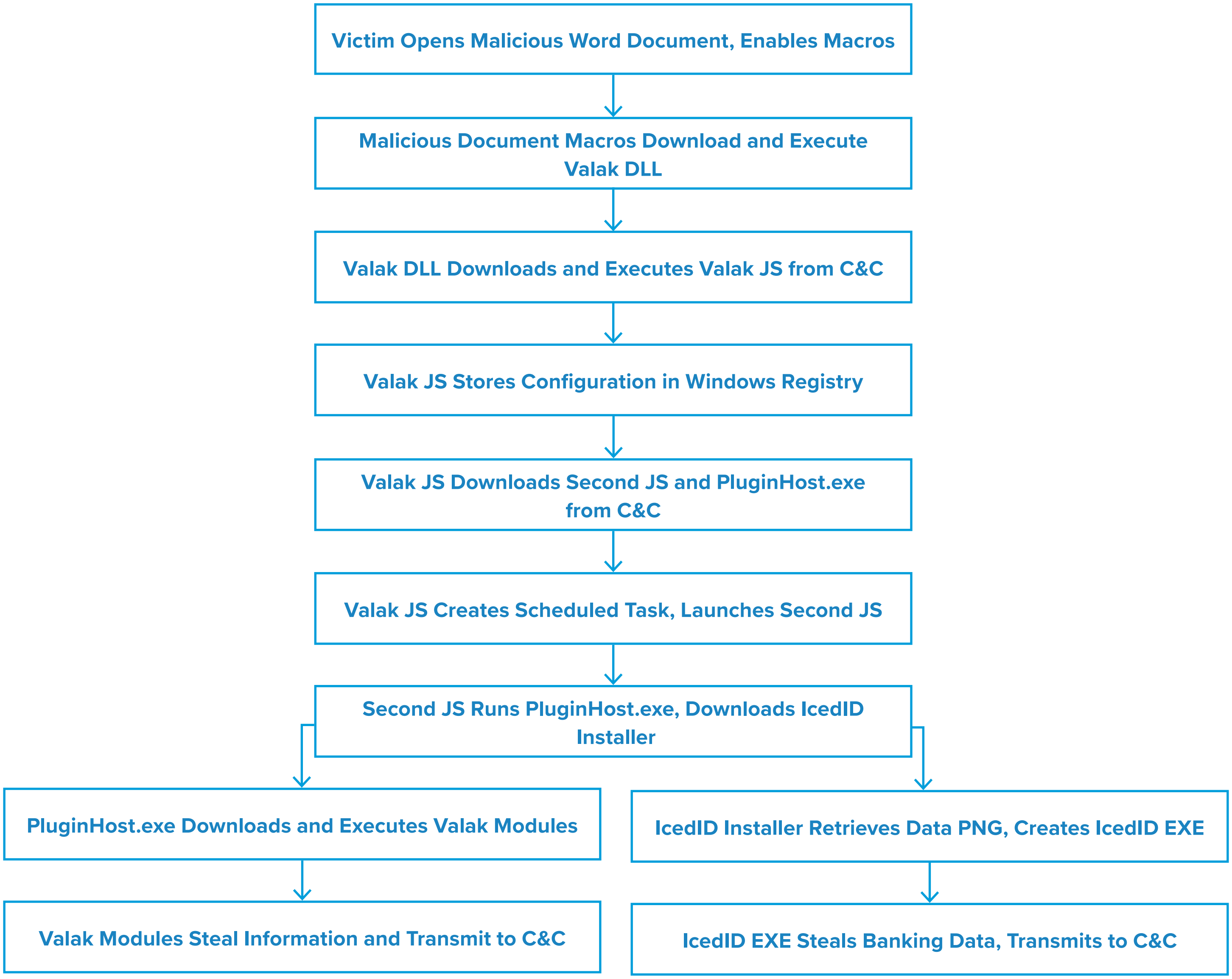
When PluginHost.exe is executed, it contacts the Valak C&C to download and install various plugin modules to expand the malware's capabilities. These modules currently include various types of reconnaissance and infostealers, but Valak may expand to include other types of modules in the future. One of Valak's most notable modules is Exchgrabber, which can steal email credentials from the infected system as well as any internal Microsoft Exchange email servers it is connected to. It then sends this information to its C&C, enabling the attacker to execute reply chain attacks using the stolen email credentials.

When the IcedID installer is executed, it retrieves a PNG image with embedded data, then uses it to generate an IcedID EXE. The IcedID EXE generates a second EXE to establish persistence, then steals banking data and transmits it to its C&C.

Vulnerabilities & Mitigation

Infoblox recommends the following actions to reduce the risk of this type of infection:

- Be aware of the possibility of reply chain attacks and do not assume that a file attachment or link is safe simply because the sender is familiar.
- Always be suspicious of vague emails, especially if there is a prompt to open an attachment or click on a link.
- If clicking on a link immediately initiates an attempt to download a file, that file is suspicious. Inspect it carefully.
- Never enable macros, and do not configure Microsoft Office to enable macros by default.

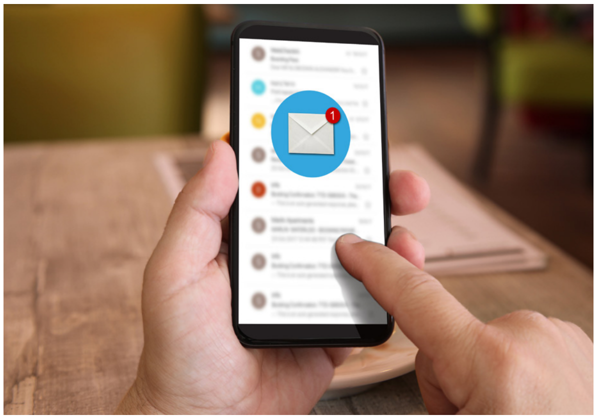

Victim Opens Malicious Word Document, Enables Macros
Malicious Document Macros Download and Execute Valak DLL
Valak DLL Downloads and Executes Valak JS from C&C
Valak JS Stores Configuration in Windows Registry
Valak JS Downloads Second JS and PluginHost.exe from C&C
Valak JS Creates Scheduled Task, Launches Second JS
Second JS Runs PluginHost.exe, Downloads IcedID Installer
PluginHost.exe Downloads and Executes Valak Modules
Valak Modules Steal Information and Transmit to C&C
IcedID Installer Retrieves Data PNG, Creates IcedID EXE
IcedID EXE Steals Banking Data, Transmits to C&C

Endnotes

1. http://malware-traffic-analysis.net/2020/06/24/index.html
2. http://malware-traffic-analysis.net/2020/06/26/index.html
3. http://malware-traffic-analysis.net/2020/06/30/index.html
4. http://malware-traffic-analysis.net/2020/07/01/index.html
5. https://www.cybereason.com/blog/valak-more-than-meets-the-eye
6. https://labs.sentinelone.com/valak-malware-and-the-connection-to-gozi-loader-confcrew/
7. https://twitter.com/malware_traffic/status/1278481732413657088

Vidar InfoStealer

Author: Nick Sundvall



Overview

From June 25 to 30, we observed a malspam email campaign distributing Vidar malware. Vidar is a trojan and infostealer that was first observed in December 2018.[1] It is a variant of the Arkei infostealer.

Customer Impact

Threat actors can reportedly purchase Vidar in online forums for $250.[2] It has the ability to steal credit cards, usernames, passwords and files, as well as take screenshots of the user's desktop.[3] It can also steal wallets for cryptocurrencies such as Bitcoin and Ethereum.

Two-factor authentication (2FA) is an additional security layer for user accounts, typically requiring a one-time use code in addition to a password to sign in to an account. Vidar specifically targets the 2FA software Authy in order to bypass this added hurdle for gaining access to an account.[2]

Campaign Analysis

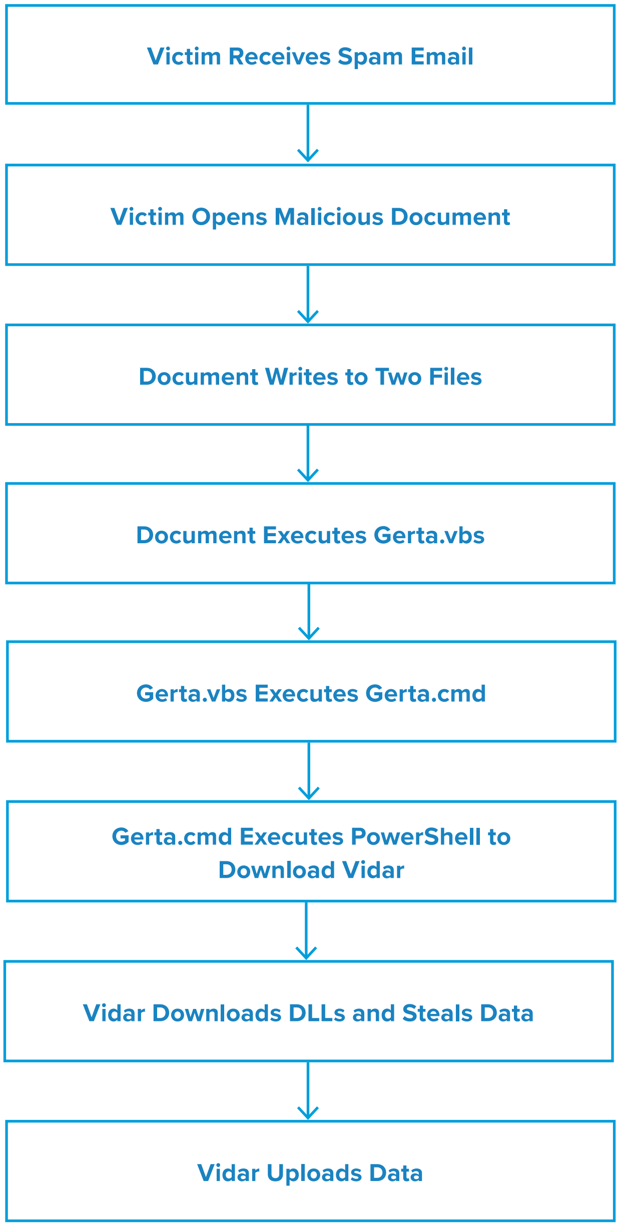
In this campaign, the threat actor sent emails with multiple subjects referencing a successful payment, such as "Confirmation of Payment" and "Your Transaction was Approved." Each email had a generic message body that resembled an invoice, with "Payment receipt attached" at the end. Every email we observed had an attached DOC file named *25.06Feo.doc*.

Attack Chain

Unlike typical malspam attacks, wherein the malware runs when the user opens the file, Vidar does not execute until the user closes the file. The attached DOC file uses the Visual Basic for Applications (VBA) method *Document_close()* to write two files - *Gerta.vbs and Gerta.cmd* - into *C:\programdata*. It executes *Gerta.vbs*, which runs *Gerta.cmd*, then launches a PowerShell script.

Throughout their execution, the scripts utilize many "sleep" commands, presumably as an anti-analysis technique to appear inactive. The PowerShell then downloads and runs the executable file *Poserto.exe*.

From here, Vidar downloads several DLL files that it uses for stealing the data. Vidar then grabs all of the data it can access, puts it in a ZIP file, and sends it back to its C&C. After sending the data, Vidar deletes itself from the infected computer.


Victim Receives Spam Email
Victim Opens Malicious Document
Document Writes to Two Files
Document Executes Gerta.vbs
Gerta.vbs Executes Gerta.cmd
Gerta.cmd Executes PowerShell to Download Vidar
Vidar Downloads DLLs and Steals Data
Vidar Uploads Data

Vulnerabilities & Mitigation

Malspam email campaigns are a common distribution method for Vidar. Infoblox therefore recommends the following precautions to reduce the possibility of infection:

- Exercise caution if it is necessary to open emails with generic subject lines.
- Always be suspicious of unexpected emails, especially regarding financial or delivery correspondence, documents, or links.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.
- Never configure Microsoft Office to enable macros by default. Many malware families use macros as an infection vector.
- Do not enable macros in Microsoft Office attachments, especially if the file's only apparent contents are directions to enable macros.

Endnotes

1. https://any.run/malware-trends/vidar
2. https://fumik0.com/2018/12/24/lets-dig-into-vidar-an-arkei-copycat-forked-stealer-in-depth-analysis/
3. https://isc.sans.edu/forums/diary/What+data+does+Vidar+malware+steal+from+an+infected+host/25398/

August 2020

Threat Reports & Cyberthreat Alerts

The Return of Emotet

Author: Eric Patterson

Overview

On July 17, Proofpoint's threat research team observed a malspam campaign featuring the return of the Emotet malware after a five-month hiatus. This was a sizable campaign that included nearly a quarter million malspam messages.[1] While the scope of this campaign differs from our previous report on Emotet,[2] the tactics and techniques it uses are largely the same.

Customer Impact

Threat actors use Emotet to steal stored passwords, sensitive banking data and browser histories from victims' computers.

The threat actors behind Emotet have repeatedly evolved the malware over time, including supplementing its native banking trojan functionality with third party tools that help to increase the malware's capabilities, such as Qakbot,[3] Trickbot[4] or IcedID.[5]

Emotet's capabilities may vary depending on the additional malware that the threat actor chooses to deliver, but they typically involve some form of credential stealer along with modules that allow the threat actor to expand the scope of their attack. These modules may include network exploits that allow the threat to move laterally within an organization's network, as well as address book harvesters that can be used to identify targets for future malspam campaigns.

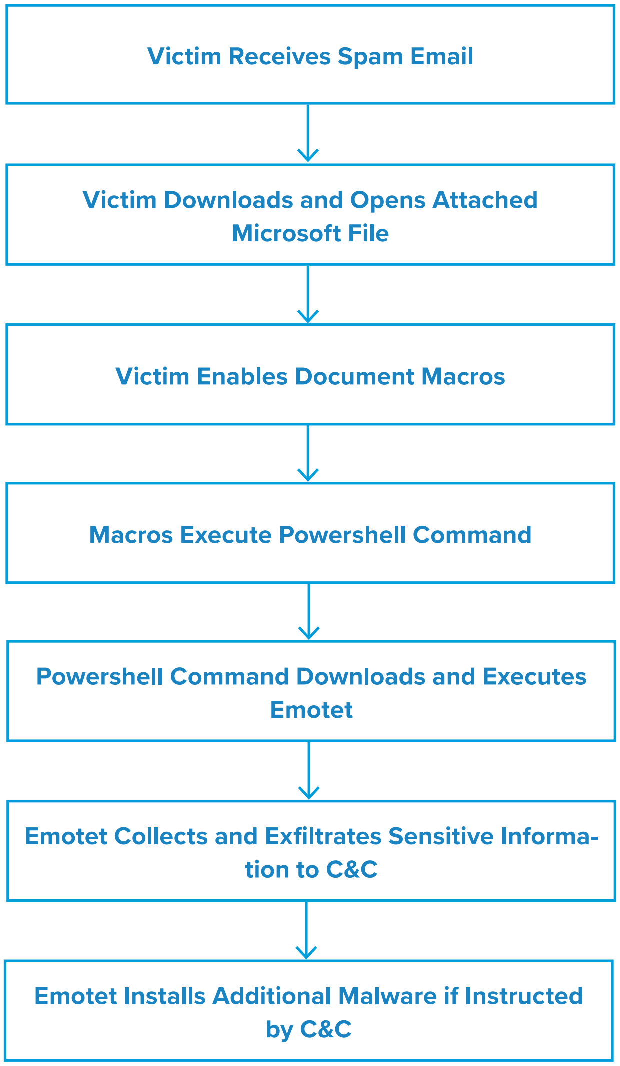
Campaign Analysis

The email lures observed in this campaign are simple in nature and are similar to lures that Emotet has previously used. The subject lines are largely generic terms like "Re:" or "Invoice#" followed by a series of numbers, but some also include the names of targeted organizations. Message bodies are generic and reference an attachment that the user must open. The attachments are Microsoft Office documents (e.g. Word or Excel) with filenames themed after common business documents like payroll and resumes.

Attack Chain

When the user opens the attached document, they are directed to enable macros. Once the user enables macros, the macros execute a Powershell (*powershell.exe*) command that attempts to download the Emotet payload (*WFSR.exe*) from one of five Base64-encoded domain names embedded in the command. If this download is successful then the Powershell command proceeds to execute the Emotet payload.

Upon execution, Emotet attempts to steal sensitive information from the victim and exfiltrate this data to one of its C&C servers. After stealing the victim's information Emotet will typically attempt to install additional malware, but it is currently unclear what additional payloads this particular campaign may be delivering.


Victim Receives Spam Email
Victim Downloads and Opens Attached Microsoft File
Victim Enables Document Macros
Macros Execute Powershell Command
Powershell Command Downloads and Executes Emotet
Emotet Collects and Exfiltrates Sensitive Information to C&C
Emotet Installs Additional Malware if Instructed by C&C

Vulnerabilities & Mitigation

Emotet is distributed via spam emails, so many of the generic precautions regarding malspam apply. Infoblox recommends the following actions to reduce the risk of this type of infection:

- Regularly train users to be aware of potential phishing efforts and how to handle them appropriately.
- A subject line or email body with the user's name does not increase the validity of the message. Likewise, just because an email appears to be part of an existing thread does not mean it is; if it does not seem to fit the context of the discussion, treat the message as a potential phish.
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Never enable macros and do not configure settings to enable macros by default. They are a common infection vector that many families of malware use.
- Never click on URLs in emails from unknown sources.
- Ensure the system's file sharing capability is closed and protected with a strong password.

Endnotes

1. https://www.proofpoint.com/us/blog/security-briefs/emotet-returns-after-five-month-hiatus
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--53
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--68
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--77
5. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--78

Qakbot InfoStealer

Author: James Barnett

Overview

On August 3, security researcher Brad Duncan reported a malspam campaign[1] that used compressed Visual Basic Script (VBScript) files to deliver Qakbot malware.

Customer Impact

Qakbot, also known as Qbot, is an infostealer that can steal a victim's credentials, banking information and files. Qakbot includes worm capabilities that allow it to spread itself to other systems on the same network, as well as rootkit capabilities that help to hide its presence and establish persistence on infected clients.

Campaign Analysis

The malspam emails in this Qakbot campaign used a variety of seemingly unrelated lures for their subject lines and body text. The one common feature of these emails was that they all enticed the recipient to click a link labelled "OPEN THE DOCUMENT".

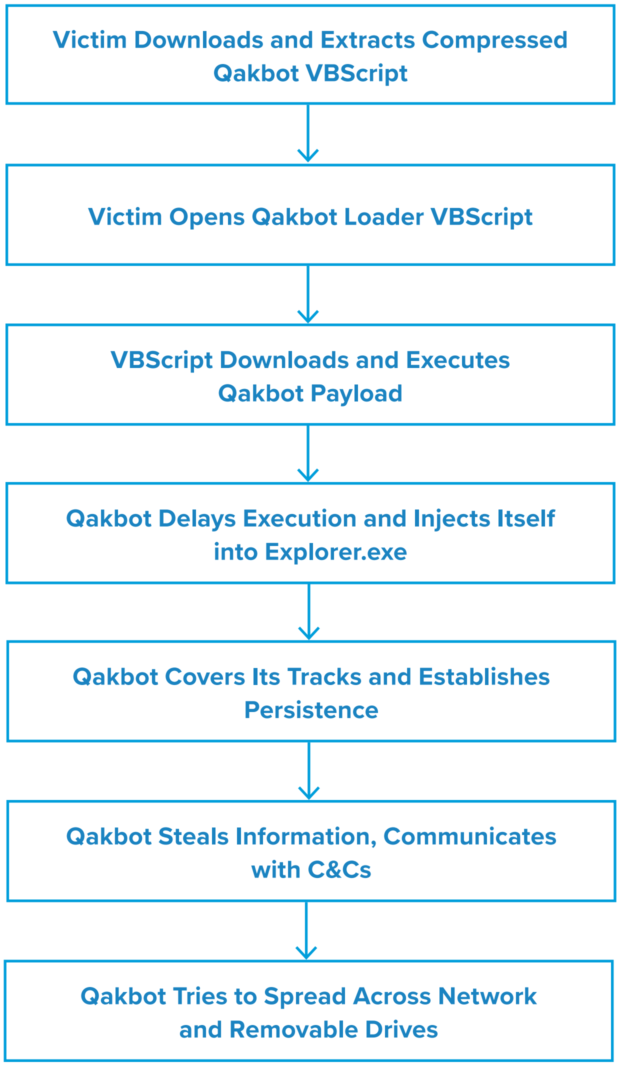
These links led to compromised websites hosting compressed archives that contained malicious VBScript files. This differs from the last Qakbot campaign we reported on, which used Microsoft OneDrive to host compressed archives that contained malicious Microsoft Word documents.[2]

Attack Chain

When the victim extracts and opens the malicious VBScript contained within the ZIP file, it will download and execute the Qakbot payload from a predetermined URL.

Between December 2019 and April 2020, Qakbot payload URLs were known to use one of two filenames: *44444.png* or *444444.png*. In this campaign, the payload URLs used a new filename: *8888888.png*. Despite their PNG file extensions, these Qakbot payloads are always Windows executable (EXE) files.

When Qakbot is executed, it remains inactive for a variable number of minutes in order to evade sandbox detection. Once active, it opens an instance of *explorer.exe* and injects the QakBot DLLsinto the process. It then attempts to cover its tracks by overwriting the original contents of the malware with one of several legitimate Windows executables.


Victim Downloads and Extracts Compressed Qakbot VBScript
Victim Opens Qakbot Loader VBScript
VBScript Downloads and Executes Qakbot Payload
Qakbot Delays Execution and Injects Itself into Explorer.exe
Qakbot Covers Its Tracks and Establishes Persistence
Qakbot Steals Information, Communicates with C&Cs
Qakbot Tries to Spread Across Network and Removable Drives

Once Qakbot finishes its attempt to cover its tracks, it creates a registry entry that will automatically launch the malware every time the computer boots up. It also creates recurring tasks to ensure that the malware is still running and has not been removed.

After establishing persistence, Qakbot begins to steal the victim's information and transmits the stolen data to its C&C servers. It also attempts to spread itself to other systems via network shares and removable drives.

Vulnerabilities & Mitigation

Infoblox recommends the following actions to reduce the risk of a Qakbot infection:

- Always be suspicious of vague emails, especially if there is a prompt to open an attachment or click on a URL or clickable text.
- Never click on URLs in emails from unknown sources.
- If clicking on a link immediately initiates an attempt to download a file, that file is suspicious. Inspect it carefully before opening it.
- Never enable macros, and do not configure Microsoft Office to enable macros by default. Macros are a very common infection vector used by many families of malware.
- Do not enable macros in Microsoft Office attachments, especially if the file's only apparent contents are directions to enable macros.
- Disable AutoRun/AutoPlay.
- Ensure File Shares are closed and protected with a strong password.

Endnotes

1. http://malware-traffic-analysis.net/2020/08/03/index.html
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--68

MassLogger InfoStealer Malspam Campaign

Author: Nick Sundvall

Overview

On August 11, we observed a malspam email campaign distributing MassLogger malware. MassLogger is a relatively new infostealer that was reportedly first observed in April 2020.[1] It is written using .NET, a programming framework developed by Microsoft.[2]

Customer Impact

The creators of MassLogger frequently update the malware, which attracts amateur threat actors because it is easy to use and offers a wide variety of features.[3]

MassLogger has the ability to log keystrokes and clipboard data, take screenshots, as well as steal credentials from Chrome, Firefox, Outlook, Thunderbird, Discord, NordVPN, FileZilla, Telegram and more.

MassLogger can also be spread over USB by injecting copies of its code into files on connected USB devices. When a user opens one of these infected files, the malicious code runs and can infect a new computer.[4]

Campaign Analysis

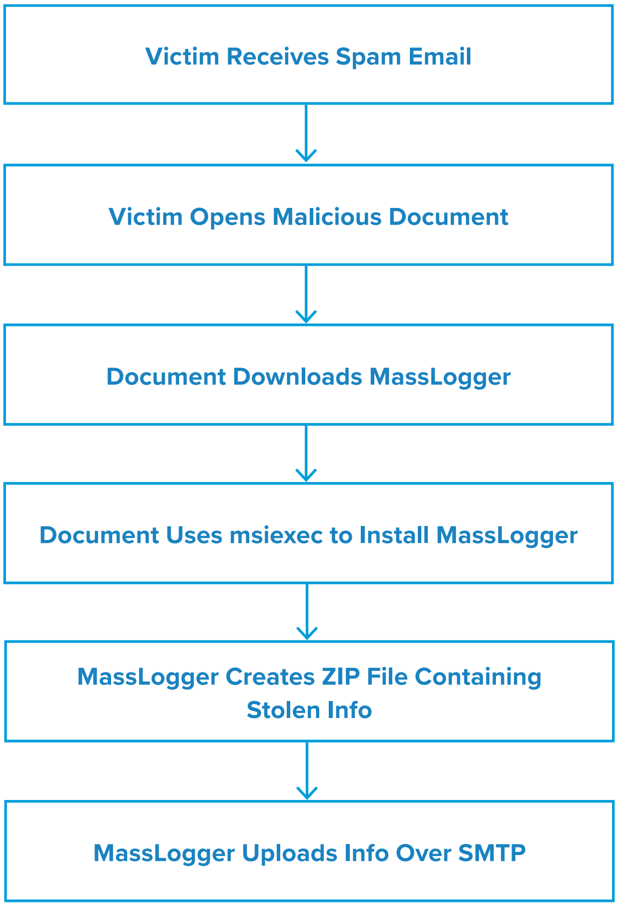
In this campaign, the threat actor sent emails with the subject “Arrival notice 203517024.” The body contained a vague message referencing an attached document, and included a legitimate link to the website for a real shipping company named Maersk. The attached file was named *DB_aabfjgideha0x0CA1.doc*, and although it has the .doc extension, it is actually a Rich Text Format (RTF) file.

Attack Chain

When the victim opens the attached file, an Object Linking and Embedding (OLE) object runs a command to download and install a Microsoft Installer file (MSI). After downloading the file, the command uses *msiexec* to install MassLogger.

From here, MassLogger begins creating a file of stolen information to exfiltrate. It sends a GET request to *api.ipify[.]org* to get the external IP address of the infected computer, as well as takes a screenshot of the user’s desktop. This site is a legitimate tool that can return public IP addresses; however, threat actors misuse it for malicious purposes in malspam attacks.

MassLogger then uses Simple Mail Transfer Protocol (SMTP) to send the stolen data and desktop screenshot in a ZIP file to an email address. In this case, the threat actor uses port 26 for SMTP rather than the usual port 25.


Victim Receives Spam Email
Victim Opens Malicious Document
Document Downloads MassLogger
Document Uses msiexec to Install MassLogger
MassLogger Creates ZIP File Containing Stolen Info
MassLogger Uploads Info Over SMTP

To maintain persistence, MassLogger writes itself to the file *C:\Users\<user>\AppData\ Roaming\mkpHrcrclaZyb.exe*. It creates a task in the Task Scheduler that sets *LogonTrigger* to Enabled, thereby ensuring that it will run every time the user logs in.

Vulnerabilities & Mitigation

Malspam email campaigns are a common distribution method for MassLogger. Infoblox therefore recommends the following precautions to reduce the possibility of infection:

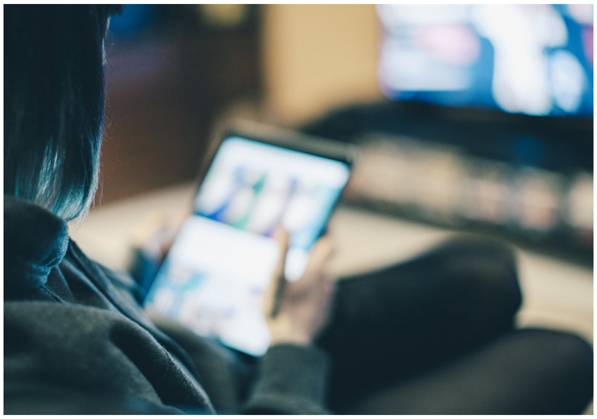
- Always be suspicious of vague emails, especially if there is a prompt to open an attachment or click on a URL or clickable text.
- Exercise caution if it is necessary to open emails with generic subject lines.
- Do not enable macros in Microsoft Office attachments, especially if the file's only apparent contents are directions to enable macros.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.

Endnotes

1. https://www.vmray.com/cyber-security-blog/malware-analysis-spotlight-massloggers-noisy-stealing-attempts/
2. https://www.fireeye.com/blog/threat-research/2020/08/bypassing-masslogger-anti-analysis-man-in-the-middle-approach.html
3. https://cofense.com/new-mass-logger-malware-massive/
4. https://www.seqrite.com/blog/masslogger-an-emerging-spyware-and-keylogger/

njRAT Malspam Campaign

Author: Eric Patterson



Overview

On August 24, a malspam email campaign distributed the njRAT malware, also known as Bladabindi and Njw0rm. njRAT is a remote access trojan (RAT) and infostealer that was first observed in January 2013[1,2,3]

In a previous campaign we reported on in May 2019, njRAT also delivered the Agent Tesla keylogger as part of its attack chain.[4]

Customer Impact

njRAT is capable of maintaining persistence and operating undetected on victims' machines while transmitting sensitive information back to its C&C infrastructure for extended periods of time. njRAT's availability, ease of use and rich feature set make it a popular choice for threat actors of all skill levels. Its known capabilities include:

- Collecting information about the system, including usernames and passwords, as well as other personal and confidential information
- Activating webcams
- Capturing screenshots
- Logging keystrokes
- Installing and uninstalling software
- Loading other plugins
- Manipulating files
- Propagating to external media
- Detecting and evading sandbox environments

Because njRAT maintains persistence and can download files, it also has the ability to download additional malware to victims' machines.

Campaign Analysis

While the exact email lures the threat actors used for distribution are unknown, njRAT has historically used messages with payment/ invoice-related themes. With these types of lures, both the subject line and email body contain messages asking the recipient to review the attached invoice or payment notice.

The attachment is a Microsoft Office Excel Macro (.xlsm) enabled file named with a 40-character alphanumeric string, mimicking that of a secure hash algorithm-1 (SHA1) convention.

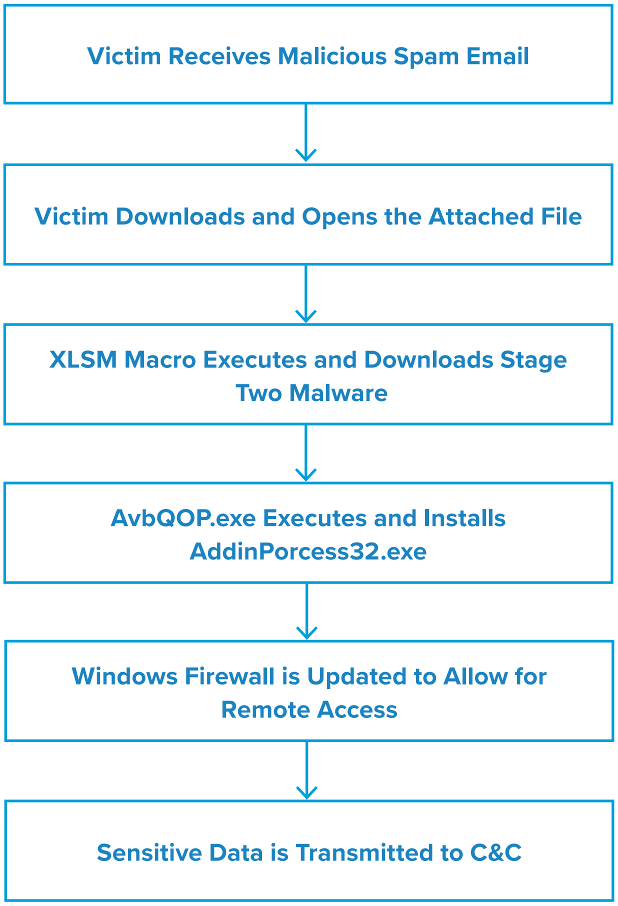
Attack Chain

When the recipient opens the email and downloads the attached .xlsm file, it prompts them to enable content. Once the recipient enables content, the underlying macro code will execute and attempt to retrieve the executable file *AvbQOP.exe*.

If successfully downloaded, *AvbQOP.exe* will execute two variants of *addinprocess32.exe*. The first is the legitimate Microsoft file that is part of the .NET framework, and the second is the njRAT malware designed to mimic the legitimate process.

Once run, njRAT will update the local firewall to add *C:\Users\admin\AppData\Local\Temp\AddInProcess32.exe* to the allowedprogram field to ensure remote connectivity. njRAT then begins to transmit sensitive data such as system information or user passwords back to its C&C infrastructure via *addinprocess32.exe*.

When remote access is achieved, threat actors will then be able to carry out any number of actions against the victim machine, including downloading additional malware, if they choose.



Victim Receives Malicious Spam Email

Victim Downloads and Opens the Attached File

XLSM Macro Executes and Downloads Stage Two Malware

AvbQOP.exe Executes and Installs AddinPorcess32.exe

Windows Firewall is Updated to Allow for Remote Access

Sensitive Data is Transmitted to C&C

Vulnerabilities & Mitigation

Infoblox recommends the following practices to prevent infection by malware distributed by spam email campaigns:

- Regularly train users to be aware of potential phishing efforts and how to handle them appropriately.
- Use an anti-spam filter for email systems.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.
- Do not open an email from the spam folder; it may be spoofed and could have triggered the filter on a characteristic that is not immediately visible.
- Always be suspicious of vague emails, especially if there is a prompt to open an attachment or click on a URL or clickable text.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g. by phone or in person) before opening them.

Endnotes

1. https://any.run/malware-trends/njrat
2. https://app.any.run/tasks/7a0563a0-9270-4de9-a3f6-6a3e297c606e/
3. https://any.run/report/0859C&C6fd38d388dea87430e57c93c5fb4da7b978b2cbd746c4b20eb468d0008/a0563a0-9270-4de9-a3f6-6a3e297c606e
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--14

Cyberthreat Advisory:
HIDDEN COBRA: BLINDINGCAN RAT Variants

Author: Eric Patterson

Executive Summary

On August 19, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA) released a Malware Analysis Report (MAR) on malware variants, dubbed BLINDINGCAN, used by the North Korean government.[1] Malicious cyber activities associated with the North Korean government are commonly referred to as HIDDEN COBRA.

BLINDINGCAN refers to a series of Remote Access Trojan (RAT) variants currently in use by HIDDEN COBRA actors to maintain persistent access inside victim infrastructure. The current target set for this campaign includes government contractors who deal with key military and energy technologies. The threat actors made use of active job postings from contractors of interest as lures to deliver one of the malware variants to the victim.

Analysis: BLINDINGCAN RAT Variants

The MAR reported four documents being delivered via email with attached Microsoft Word Document (.docx) files purporting to reference open job postings for targeted companies. The DOCX files contain a series of Extensible Markup Language (XML) files in a directory structure that when opened and depending on the file received, attempt to contact one of two C&C domains:

- hxxps://agarwalpropertyconsultants[.]com/assets/form/template/img/boeing_ia_cm.jpg
- hxxps://www[.]anca-aste.it/uploads/form/boeing_iacm_logo.jpg

Depending on the information gathered from the victim's system, a 32- or 64-bit stage-one UPX- packed DLL payload will be downloaded to the victim: machine– d40ad4cd39350d718e189adf45703eb3a3935a7cf8062C&C0c663bc14d28f78c9 or 0fc12e03ee93d19003b2dd7117a66a3da03bd6177ac6eb396ed52a40be913db6, respectively.

Once installed, the follow-on execution chains appear identical for both the 32- and 64-bit variants. The stage-one payloads decode themselves using a hardcoded 0x59 XOR key, and install and execute the DLL in C:\ProgramData\iconcache.db. Stage-two payloads consist of a secondary 32- or 64-bit UPX-packed DLL run out of C:\ProgramData\iconcache.db. During execution, it decompresses two additional DLL files into memory: one is the HIDDEN COBRA RAT variant, and the other is designed to unmap the DLL from memory.

Both of the HIDDEN COBRA RAT variants decrypt themselves using a different hard-coded AES key before attempting to collect the following system information:

- Operating system (OS) version information
- Processor information
- System name
- Local IP address information
- Media access control (MAC) address
- User-agent string (UAS)

This information will be transmitted to one of two C&C domains: curiofirenze[.]com or automercado[.]co[.]cr. The malware will then craft a series of HTTP POST requests to its C&C using four distinct Base64-encoded parameters that relate to built-in functions capable of being executed on the victim machine. The functions of the malware include:

- Retrieve information about all installed disks, including the disk type and the amount of free space on the disk
- Create, start and terminate a new process and its primary thread
- Search, read, write, move and execute file
- Get and modify file or directory timestamps
- Change the current directory for a process or file
- Delete malware and artifacts associated with the malware from the infected system

Prevention and Mitigation

The Cybersecurity and Infrastructure Security Agency (CISA) recommends the following mitigation techniques to defend against BLINDINGCAN. CISA also recommends that any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Endnotes

1. https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a

Cyberthreat Advisory: HIDDEN COBRA: BeagleBoyz and FASTCash 2.0

Executive Summary

On August 16, the Cybersecurity and Infrastructure Security Agency (CISA) published a joint advisory based on analytic efforts with the Department of the Treasury (Treasury), the Federal Bureau of Investigation (FBI), U.S. Cyber Command (USCYBERCOM) and government partners.[1] The report describes tools and techniques used by an element of the North Korean government to carry out attacks against automated teller machines (ATMs), efforts the U.S. government refers to as “FASTCash 2.0: North Korea’s BeagleBoyz Robbing Banks.”

Malicious cyberactivities associated with the North Korean government are commonly referred to as HIDDEN COBRA. The BeagleBoyz is a hacking group that robs banks via remote internet access, and their activity is a subset of HIDDEN COBRA. According to CISA’s report, the BeagleBoyz “overlap to varying degrees with groups tracked by the cybersecurity industry as Lazarus, Advanced Persistent Threat 38 (APT38), Bluenoroff, and Stardust Chollima.” The United Nations (UN) considers the BeagleBoyz’ activity a means to circumvent UN resolutions and generate funds to support prohibited nuclear weapons and ballistic missile programs.

The BeagleBoyz group is part of North Korea’s Reconnaissance General Bureau, and has been carrying out FASTCash campaigns against the retail payment infrastructure of banks since 2016. Since CISA’s 2018 report on it, there have been two significant changes: the use of FASTCash against banks that are hosting switch[2] applications on Windows servers, and the targeting of interbank payment processors. The group has also attacked cryptocurrency exchanges to convert the stolen funds into fiat currency.

The report profiles the group, lists its known current and historical targets, provides technical analysis of its known tools and techniques, and incorporates the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework.

Analysis

Pre-Infection

BeagleBoyz uses many techniques to gain initial access to victim computers, including spear phishing and job application-themed phishing, watering holes and drive-bys, exploiting weaknesses in public facing applications, stealing credentials, using external remote services, and breaching an organization that has a trusted relationship with the ultimate target.

The report authors also assess that BeagleBoyz may collaborate with or employ criminal hacking groups such as TA505 as part of its efforts to gain access to victims.

Post-Infection

BeagleBoyz is selective in terms of which systems it exploits after it gains initial access. The group uses a variety of techniques to escalate its privileges, establish persistence and evade detection.

CISA's report provides a link to a technical report about an infostealer referred to as ELECTRICBANDWAGON,[3] which is used to log and encrypt data, as well as capture screenshots, but does not have network functionality. This malware is reportedly only one of several techniques that BeagleBoyz uses to steal credentials. When available,the group also appears to favor legitimate administrative tools such as Powershell for reconnaissance.

The North Korean group appears to search for two things once it has gained access to a financial institution: the SWIFT terminal and the payment switch application server. Once found, the group uses the stolen credentials to move laterally in the corporate network and access those systems.

BeagleBoyz has used multiple tools over the years to maintain access to and interact with victim networks, including remote access trojans (RATs) such as CROWDEDFLOUNDER, HOPLIGHT and COPPERHEDGE for cryptocurrency exchange exploitation. It has also used network proxy tunneling tools such as VIVACIOUSGIFT and ELECTRICFISH. Full technical reports of these malware are available at https://us-cert.cisa.gov/northkorea.

FASTCash

FASTCash malware can reply to financial request messages with ISO 8583 format affirmative responses that are not legitimate despite their appearance. BeagleBoyz has both UNIX[4] and Windows versions of the malware.

FASTCash for UNIX

FASTCash for UNIX is made up of AIX executable files that use process injection. One of the executables enables an application to manipulate transactions on financial systems using the ISO 8583 international standard for financial transaction card-originated interchange messaging. The injected executables interpret financial request messages and construct fraudulent financial response messages.

FASTCash for Windows

FASTCash for Windows also manipulates ISO 8583 messages by injecting itself into software already running on Windows, and then taking over the software's network send and receive functions. However, it checks incoming messages for specific information, possibly certain account numbers, and if it finds it, the malware sends a fraudulent response that will not be processed by the switch application and therefore, not raise suspicion of the transaction.

The report indicates that two variants of this version have been identified: one supports ASCII encoding, the other supports Extended Binary Coded Decimal Interchange Code (EBCIDC) encoding.

Prevention and Mitigation

CISA's report outlines recommendations for institutions with retail payment systems, organizations with ATM point of sale devices, as well as for all organizations. We are providing them all below directly.

Recommendations for Institutions with Retail Payment Systems

Require chip and personal identification number (PIN) cryptogram validation.

- Implement chip and PIN requirements for debit cards.
- Validate card-generated authorization request cryptograms.
- Use issuer-generated authorization response cryptograms for response messages.
- Require card-generated authorization response cryptogram validation to verify legitimate response messages.

Isolate payment system infrastructure.

- Require multi-factor authentication for any user to access the switch application server.
- Confirm perimeter security controls prevent internet hosts from accessing the private network infrastructure servicing your payment switch application server.
- Confirm perimeter security controls prevent all hosts outside of authorized endpoints from accessing your system, especially if your payment switch application server is internet accessible.

Logically segregate your operating environment.

- Use firewalls to divide your operating environment into enclaves.
- Use access control lists to permit/deny specific traffic from flowing between those enclaves.
- Give special considerations to segregating enclaves holding sensitive information (e.g., card management systems) from enclaves requiring internet connectivity (e.g., email).

Encrypt data in transit.

- Secure all links to payment system engines with a certificate-based mechanism, such as Mutual Transport Layer Security, for all external and internal traffic external.
- Limit the number of certificates that can be used on the production server and restrict access to those certificates.

Monitor for anomalous behavior as part of layered security.

- Configure the switch application server to log transactions and routinely audit transaction and system logs.
- Develop a baseline of expected software, users, and logons and monitor switch application servers for unusual software installations, updates, account changes or other activities outside of expected behavior.
- Develop a baseline of expected transaction participants, amounts, frequency and timing. Monitor and flag anomalous transactions for suspected fraudulent activity.
- **Recommendations for Organizations with ATM or Point of Sale Devices**

Validate issuer responses to financial request messages.

- Implement chip and PIN requirements for debit cards.
- Require and verify message authentication codes on issuer financial request response messages.
- Perform authorization response cryptogram validation for chip and PIN transactions.
- **Recommendations for All Organizations**

Users and administrators should use the following best practices to strengthen the security posture of their organization’s systems:

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up to date.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users’ ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators’ group unless required.
- Enforce a strong password policy and require regular password changes.
- Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations and configure it to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its “true file type” (i.e., the extension matches the file header).

- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the internet before executing.
- Maintain situational awareness of the latest threats.
- Implement appropriate access control lists.

Endnotes

1. https://us-cert.cisa.gov/ncas/alerts/aa20-239a
2. "Switch is a tool that facilitates communication between different payment service providers. It typically provides a merchant-driven rules-based authorization and switching solution. It dynamically routes payment transactions between multiple acquirers and Payment Service Providers." https://lyra.com/in/what-is-payment-switch/
3. https://us-cert.cisa.gov/northkorea
4. https://www.us-cert.gov/ncas/alerts/TA18-275A

September 2020

Threat Reports & Cyberthreat Alerts

Metamorfo Banking Trojan

Author: James Barnett

Overview

On August 18, cybersecurity researchers at Menlo Security reported an ongoing malware campaign that used HTML smuggling techniques to deliver the Metamorfo banking trojan.[1]

Customer Impact

Metamorfo is a banking trojan that attempts to steal sensitive financial information and exfiltrate that data to a C&C server. What sets Metamorfo apart from other banking trojans is the wide variety of evasive techniques it uses to bypass security mechanisms and deliver its payload without being detected.

Campaign Analysis

The Metamorfo campaign in this report involved malicious links that used embedded JavaScript to construct the initial malware component within the victim's browser rather than transferring it as a traditional file download. This technique is known as HTML smuggling, and it allows threat actors to bypass security measures that are commonly used to block malicious URLs and file downloads.

While the report did not specify how this campaign distributed its malicious links, Metamorfo has used malspam as its primary distribution method in previous campaigns.[2]

Attack Chain

When the victim clicks the malicious link, they are redirected to a landing page that immediately executes an embedded JavaScript. This JavaScript uses the victim's browser to reconstruct a ZIP file containing the Metamorfo downloader on the victim's system. Because the file is created by the victim's browser rather than being transferred over the network, this method allows Metamorfo to bypass security measures that block malicious URLs and file downloads.

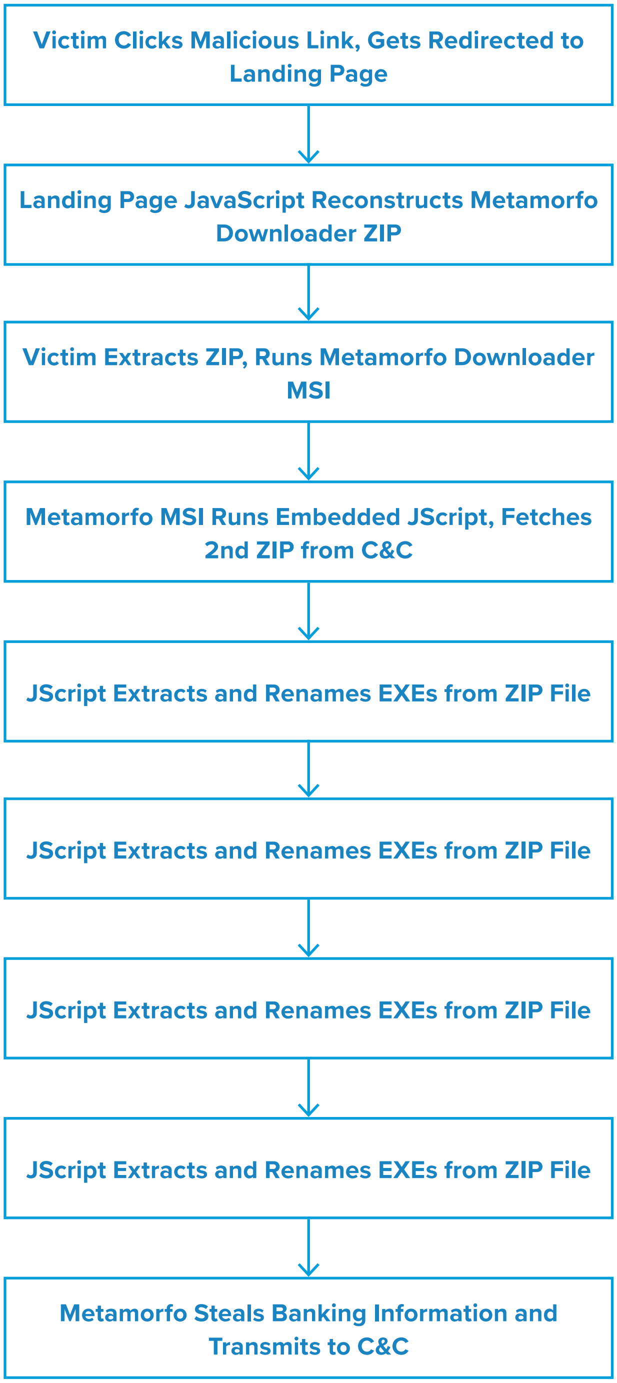
Once the JavaScript has reconstructed the ZIP file, the victim must manually extract and open the Metamorfo MSI downloader. When they do so, the downloader executes an embedded JScript that contacts the Metamorfo C&C to download a second ZIP file to the victim's Public Documents folder. This second ZIP file (*input20.jpg*) uses a misleading JPG file extension to conceal its true nature.

After downloading the second ZIP file, the Metamorfo JScript proceeds to extract two files from it. The first file, *rundll32.exe*, is a malicious Metamorfo payload and the second, *Avira.exe*, is a legitimate and digitally signed component of Avira Antivirus. The JScript randomly renames both of these files when extracting them, as well as changes the file extension of the Metamorfo payload from EXE to BMP in order to evade detection.

Once the Metamorfo JScript has extracted and renamed the EXEs from the ZIP file, it creates an LNK file that points to the renamed version of *Avira.exe* and adds it to the system's AutoRun list to establish persistence. It then executes the Metamorfo payload to download and decrypt a malicious DLL file from a remotelocation. Metamorfo saves this malicious DLL as *Avira.OE.NativeCore.dll*, which is the same name used by a legitimate DLL file packaged with Avira.

After saving the malicious DLL file, the Metamorfo JScript begins using the legitimate Avira EXE to perform a DLL hijacking attack. When the Avira EXE starts, it looks for *Avira.OE.NativeCore.dll* and loads it. Normally this behavior would be benign, but because Metamorfo has replaced the legitimate DLL with its malicious payload, the Avira EXE loads the malware instead. Using a legitimate EXE from a trusted antivirus vendor to load its malicious payload allows Metamorfo to evade detection and bypass security controls.

Once the Metamorfo DLL is loaded, the malware performs standard banking trojan activities. It monitors web visits to targeted banking institutions, logs keystrokes, searches for saved banking credentials, and takes screenshots of the victim's system. It then transfers the stolen information back to its C&C.


Victim Clicks Malicious Link, Gets Redirected to Landing Page
Landing Page JavaScript Reconstructs Metamorfo Downloader ZIP
Victim Extracts ZIP, Runs Metamorfo Downloader MSI
Metamorfo MSI Runs Embedded JScript, Fetches 2nd ZIP from C&C
JScript Extracts and Renames EXEs from ZIP File
JScript Extracts and Renames EXEs from ZIP File
JScript Extracts and Renames EXEs from ZIP File
JScript Extracts and Renames EXEs from ZIP File
Metamorfo Steals Banking Information and Transmits to C&C

Vulnerabilities & Mitigation

Infoblox recommends the following actions to reduce the risk of this type of infection:

- Never click on URLs in emails from unknown sources.
- Be wary of links in incoming emails. If a well-known company sends a message with a link, it should generally point to the company's domain (e.g. "http://fedex[.]com" if the sender is FedEx). Hover the mouse over the link to verify the true destination.
- If clicking on a link immediately initiates an attempt to download a file, that file is suspicious. Inspect it carefully before opening it.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Use browser plugins such as NoScript, which can stop malicious JavaScript loading from untrusted sources.

Endnotes

1. https://www.menlosecurity.com/blog/new-attack-alert-duri
2. https://www.fortinet.com/blog/threat-research/analysis-metamorfo-variant-targets-financial-organizations

Raccoon InfoStealer Malspam Campaign

Author: Nick Sundvall

Overview

On September 1, we observed a malspam email campaign distributing Raccoon malware. Raccoon, also known as Racealer, is an infostealer that was first observed in April 2019.[1]

Customer Impact

Raccoon can steal credit cards, usernames, passwords and cryptocurrency wallets.[2] Although it has relatively basic features, it is effective and affordable.

Threat actors can reportedly purchase Raccoon from online forums for $75, a reportedly lower-than-average price for similar types of malware.[3] Raccoon is a Malware-As-A-Service (MaaS) that allows buyers to receive software updates and support from the sellers.

Campaign Analysis

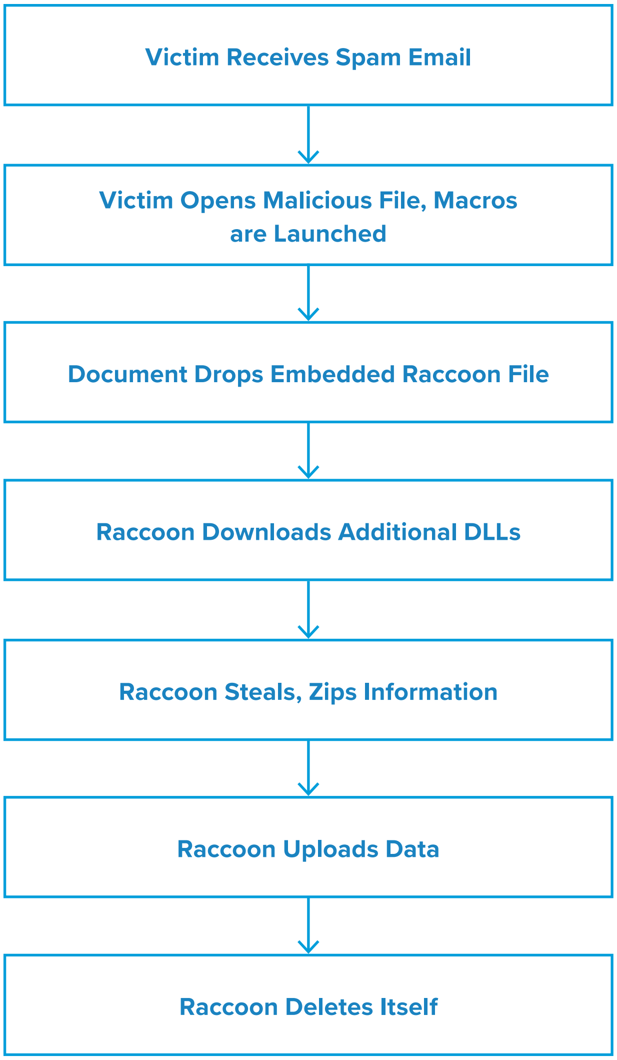
In this campaign, the threat actor sent emails with the vague subject Purchase Order. The emails contained a message body beginning "Dear Sir, Pls find enclosed our new purchase order for your reference." Each email had an attached file named *Purchase Order.xlsx*.

Attack Chain

The XLSX file had been archived in OpenXML format, which enabled the threat actor to include additional files containing macros in the archive. Opening the attached file unzips the archive. From here, the XLSX file had access to the additional files in the archive containing the malicious macro.[4]

Once the macros were enabled, the malware exploited CVE-2017-11882[5]—a memory corruption vulnerability in Microsoft Office's Equation Editor—to drop *RichX.com*, an embedded executable file that is the final Raccoon payload.

Raccoon then downloaded multiple DLL files that it used for stealing data. Once it stole and zipped all of the targeted information, Raccoon sent it back to its C&C server. Finally, Raccoon launched *cmd.exe* to delete itself from the victim's computer.


Victim Receives Spam Email
Victim Opens Malicious File, Macros are Launched
Document Drops Embedded Raccoon File
Raccoon Downloads Additional DLLs
Raccoon Steals, Zips Information
Raccoon Uploads Data
Raccoon Deletes Itself

Vulnerabilities & Mitigation

Malspam email campaigns are a common distribution method for Raccoon. Infoblox therefore recommends the following precautions to reduce the possibility of infection:

- Never configure Microsoft Office to enable macros by default. Many malware families use macros as an infection vector.
- Do not enable macros in Microsoft Office attachments, especially if the file's only apparent contents are directions to enable macros.
- Always be suspicious of unexpected emails, especially regarding financial or delivery correspondence, documents or links.
- Exercise caution if it is necessary to open emails with generic subject lines.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.

Endnotes

1. https://www.cyberark.com/resources/threat-research-blog/raccoon-the-story-of-a-typical-infostealer
2. https://blog.trendmicro.com/trendlabs-security-intelligence/raccoon-stealers-abuse-of-google-cloudservices- and-multiple-delivery-techniques/
3. https://www.cyberark.com/resources/threat-research-blog/raccoon-the-story-of-a-typical-infostealer
4. https://blog.malwarebytes.com/threat-analysis/2017/10/decoy-microsoft-word-document-deliversmalware-through-rat/
5. https://nvd.nist.gov/vuln/detail/CVE-2017-11882

Cyberthreat Advisory: APT39 Malicious Activity and Tools

Author: Nathan Toporek

Executive Summary

On September 17, the Federal Bureau of Investigation (FBI) published a new FLASH alert in coordination with the Department of Homeland Security (DHS), and the Department of the Treasury (Treasury).[1] The report describes multiple types of malware that the Iranian Rana Intelligence Computing Company—also known as APT39—has used in their global operations. In the report, the FBI included descriptions of how the various types of malware operate, as well as a set of YARA rules for each type. The FBI also published a representative set of malware samples to VirusTotal for public analysis.

Rana Intelligence Computing Company is a front company for Iran's Ministry of Intelligence and Security (MOIS). According to the FBI, it has targeted hundreds of individuals and entities in more than 30 countries spread across Asia, Africa, Europe and North America. It has previously targeted foreign citizens, foreign governments, and organizations predominantly in the travel, hospitality, academic and telecommunications industries. Specifically in Iran, it has targeted individuals and dissidents, in addition to companies and academic institutions.

Analysis

The FLASH alert describes multiple variants of malware that Rana used in its operations, including signatures for indicators of compromise (IOCs), along with sets of YARA rules that the FBI has developed to identify samples. The report includes variants of malicious Visual Basic Script (VBS), AutoIt Malware, two executables leveraging the Background Intelligent Transfer Service (BITS), an executable that mocks the Firefox web browser, a Python-based malware script, a malicious Android Package (APK) and a malicious Microsoft Cabinet file named *depot.dat*.

VBS Malware

APT39 embedded multiple VBS scripts inside Microsoft Office documents, which it sent to victims via spear phishing and other techniques that use social engineering. When a victim opens one of the documents, the VBS code will:

1. Deobfuscate and run two scripts: one PowerShell, and another VBS.
2. Configure download and upload paths on the victim's computer.
3. Set up a scheduled task to run the VBS file from step one every two minutes.
4. Run the PowerShell script from step one.
5. Communicate with a C&C server using a URL of: *<actor IP or URL>:port/update.php?req=<victim identifier>*. This URL is preceded by information specifying an action to download data, upload data, or download a batch file.

Both the VBS and the PowerShell scripts work to upload a victim's files and execute commands locally via *cmd.exe*.

AutoIt Malware

APT39 embedded multiple VBS scripts inside Microsoft Office documents, which it sent to victims via spear phishing and other techniques that use social engineering. When a victim opens one of the documents, the VBS code will:

1. Perform a DNS flush.
2. Create upload and download directories on the victim's computer.
3. Check for, then update the following registry key: *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion.*
4. Communicate with a C&C, similar to the VBS scripts in the previous section.

- **BITS 1.0 Malware**

Both the VBS and AutoIt malware download this malware, which uses Microsoft's Background Intelligent Transfer Service (BITS) to upload a victim's data to a C&C server. The FBI's analysis showed that this malware installs a dropper containing two Microsoft cabinet (CAB) files. One of them is empty, while the other contains two Microsoft executable files (EXEs), along with XML files that create and run scheduled tasks to upload victim data. The two EXE files in the CAB exfiltrate the victim's data to attacker infrastructure via BITS.

BITS 2.0 Malware

This variant is similar to the BITS 1.0 malware above in how it communicates with attacker infrastructure, but it has significant technical differences. Compared to the BITS 1.0 malware, the BITS 2.0 malware is a self-extracting executable containing an image, a VBS file, and another EXE. The VBS file creates and runs a persistent scheduled task to exfiltrate data; the EXE leverages BITS to exfiltrate data to attacker infrastructure.

Firefox Malware

This malware masquerades as a legitimate Firefox executable. It contains files and functionality that allow it to:

- Compress / decompress files
- Log keyboard activity
- Capture screenshots
- Communicate with a C&C

- **Python-Based Malware**

This Python-based malware came packaged in a Roshal Archive (RAR) file. It reaches out via HTTP to a C&C server and downloads additional malware when it runs. The FBI did not specify the nature or function of additional malware.

Android Malware

APT39 used a malicious APK named *optimizer.apk* that was designed to communicate with the C&C server *saveingone[.]com*, and can:

- Record audio
- Take photos
- Exfiltrate data to a C&C server

- **dat Malware**

The *depot.dat* malware is a Microsoft CAB file containing four DLLs that can perform keylogging, and capture screenshots of the victim's computer. A separate dropper file decrypts and achieves persistence of the files in depot.dat by overriding the *SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows* registry key.

Prevention and Mitigation

The FBI FLASH report provides the following set of recommendations to mitigate this malware:

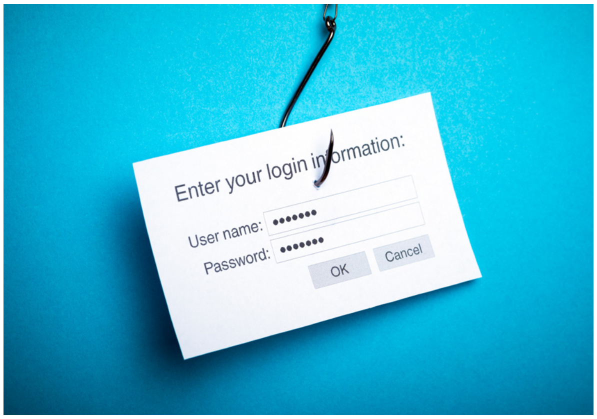
- Employ regular updates to applications and the host operating system to ensure protection against known vulnerabilities.
- Establish, and backup offline, a “known good” version of the relevant server and a regular change management policy to enable monitoring for alterations to servable content with a file integrity system.
- Employ user input validation to restrict local and remote file inclusion vulnerabilities. Implement a least-privileges policy on the Webserver to:
  - Reduce adversaries’ ability to escalate privileges or pivot laterally to other hosts.
  - Control creation and execution of files in particular directories.
- If not already present, consider deploying a demilitarized zone (DMZ) between the Web-facing systems and corporate network. Limiting the interaction and logging traffic between the two provides a method to identify possible malicious activity.
- Ensure a secure configuration of Webservers. All unnecessary services and ports should be disabled or blocked. All necessary services and ports should be restricted where feasible. This can include whitelisting or blocking external access to administration panels and not using default login credentials.
- Use a reverse proxy or alternative service to restrict accessible URL paths to known legitimate ones.
- Conduct regular system and application vulnerability scans to establish areas of risk. While this method does not protect against zero day attacks, it will highlight possible areas of concern.
- Deploy a Web application firewall and conduct regular virus signature checks, application fuzzing, code reviews and server network analysis.

Endnotes

1. https://www.ic3.gov/media/news/2020/200917-2.pdf

Malicious Spam Campaign Delivers Static Phishing Page

Author: Nathan Toporek



Overview

On September 20, Infoblox observed a malspam campaign delivering a malicious HTML file capable of phishing for credentials. While threat actor(s) used generic lures in their emails, the HTML file specifically targeted WeTransfer, a file-sharing service.

Customer Impact

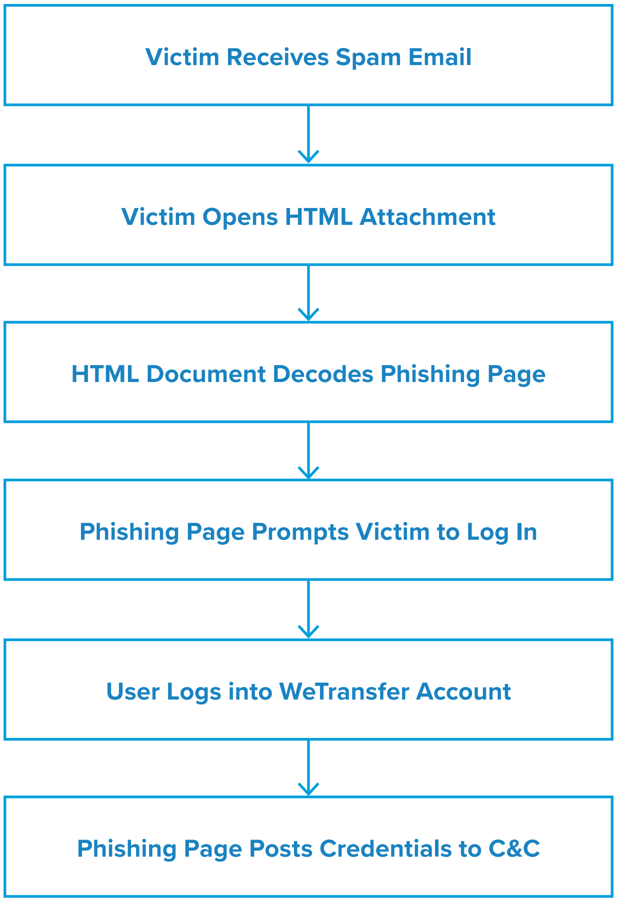
Threat actors used a malicious HTML file in this campaign that is not related to any family of malware that Infoblox is aware of. The file harvests and exfiltrates WeTransfer credentials.

Campaign Analysis

In this campaign, threat actors sent victims an email with a subject of *Request for Quotation-Urgent!!!*. While the message body was empty, the email did include an HTML file attachment named order: *Copy.html*.

Attack Chain

The HTML file contains a secondary escaped HTML page embedded in its contents. When the victim opens the attachment, it will unpack the secondary HTML page and alert the user that they are viewing a secure document and need to log in to view its contents. If the user successfully logs into the WeTransfer service, an embedded iframe within the second HTML page will collect and post credentials to an attacker-owned URL. However, if the user fails to log in, the HTML page will alert them that their credentials are invalid.


Victim Receives Spam Email
Victim Opens HTML Attachment
HTML Document Decodes Phishing Page
Phishing Page Prompts Victim to Log In
User Logs into WeTransfer Account
Phishing Page Posts Credentials to C&C

Vulnerabilities & Mitigation

This malspam campaign relies solely on social engineering tactics to persuade the victim into revealing their credentials. As such, Infoblox recommends the following precautions to reduce the possibility of compromise:

- Regularly train users to be aware of potential phishing efforts and how to handle them appropriately.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Be aware of any attachment's file type, and never open files that could be a script (.vbs, .cmd, .bat), an internet shortcut file or compression file. Using the latter is a known method for evading detection methods based on file hashes and signatures. Threat actors use them to mask the real malicious file due to email service restrictions on attachment file type.

Glupteba Backdoor Trojan

Author: Christopher Kim

Overview

From September 20 to 26, Infoblox detected communications between malicious Glupteba bots and C&C servers in customer DNS traffic. This activity was identified by our Threat Insight[1] security solution, which employs machine learning models to detect and block certain types of malicious behavior, in this case data exfiltration.[2]

Customer Impact

Glupteba is a backdoor trojan that was first discovered in 2014.[3] What sets it apart from other backdoors is its sophisticated functionality for stealthily controlling remote bots. The malware can also use modules to perform the following tasks:

- Install a rootkit to control the bot and hide malware files and processes from the system administrator.
- Turn off antivirus and security monitoring programs.
- Propagate across the victim's network using EternalBlue variant exploits.
- Compromise unpatched ethernet routers and use them as network proxies for future attacks.
- Steal data from local browser files.
- Secretly run cryptominers.

In late 2019, the malware authors applied a significant update that allows Glupteba to fetch C&C information by querying Bitcoin transaction IDs hardcoded into the binary.[4]

Campaign Analysis

Threat Insight detected 28 unique second-level domains (SLDs) in customer DNS traffic that were used for C&C communications. The domains are all inherently malicious and were registered between March and May 2020. The threat actor registered most of the domains with companies such as GoDaddy, Namecheap or 101domain. The threat actor set all the nameservers to Cloudflare, a network provider often used by miscreants for its Dynamic DNS services.

Domain names may have been generated with a dictionary-based domain generation algorithm (DGA). Each domain name is alphanumeric and consists of two or more words. Each bot submitted hundreds of DNS requests to fully qualified domain names (FQDNs) that contained a patterned global unique identifier (GUID).

Historic queries in customer DNS traffic indicated that some devices were infected as early as May 2020.

Attack Chain

In one recent campaign, the actor distributed Glupteba using a fake YouTube video download site.[5] When a visitor submits the URL of a YouTube video into the site's input field, they are prompted to download an executable file hosted at another site. The filename of the executable includes the individual words of the video title, delimited by underscores.

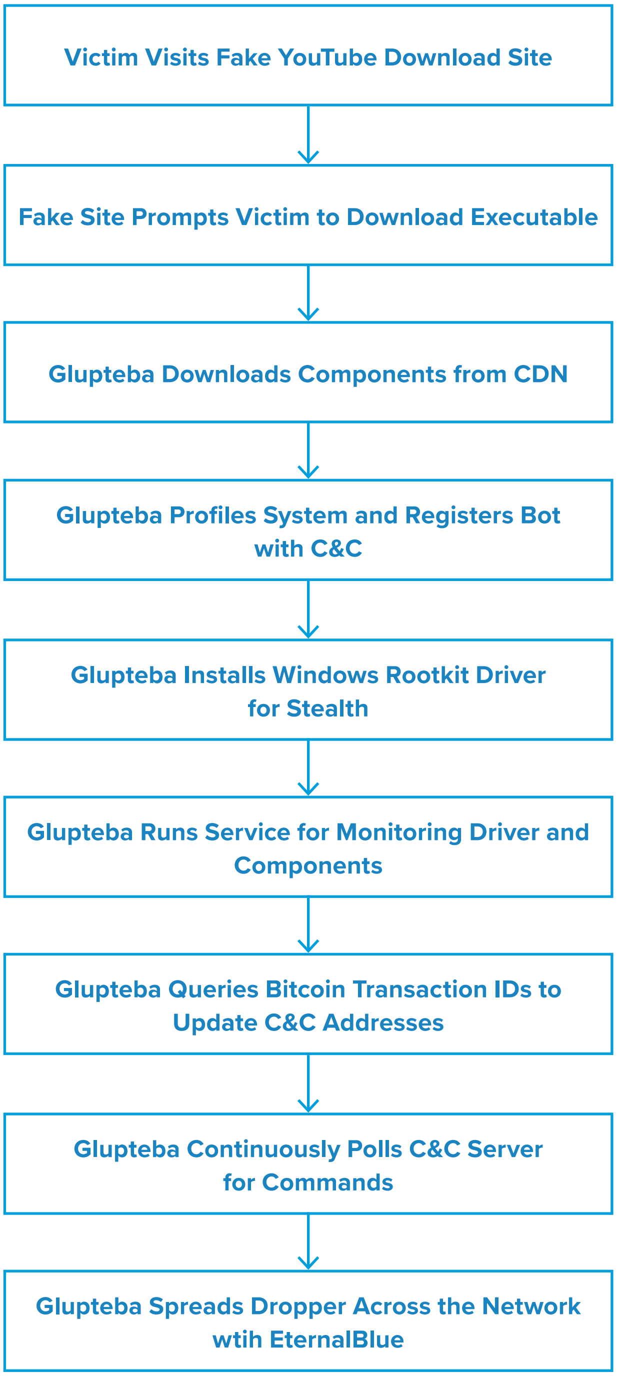
After the victim executes the file, the malware downloads components that extend its capabilities from the actor-controlled content distribution network (CDN) server.

Next, the malware profiles the infected machine and establishes a connection with the C&C to submit system information, as well as register the bot within the Glupteba botnet. Additionally, Glupteba identifies and shuts down antivirus and security monitoring applications that are running in the system.

The malware then installs a Windows kernel rootkit driver to protect certain directories and components that it dropped into the system.

Glupteba achieves persistence using the *watchdog.exe* process that reinitializes any failed driver or components of the malware. This process also updates the C&C address configuration by querying Bitcoin transaction IDs hardcoded in the binary. Throughout the process, the malware continuously polls the C&C server to obtain commands, configuration information, and other instructions.

Finally, Glupteba spreads itself laterally across the network after it identifies vulnerable machines using the EternalBlue exploit.


Victim Visits Fake YouTube Download Site
Fake Site Prompts Victim to Download Executable
Glupteba Downloads Components from CDN
Glupteba Profiles System and Registers Bot with C&C
Glupteba Installs Windows Rootkit Driver for Stealth
Glupteba Runs Service for Monitoring Driver and Components
Glupteba Queries Bitcoin Transaction IDs to Update C&C Addresses
Glupteba Continuously Polls C&C Server for Commands
Glupteba Spreads Dropper Across the Network wtih EternalBlue

Vulnerabilities & Mitigation

Infoblox recommends the following actions to reduce the risk of this type of infection:

- Subscribe to Infoblox Threat Insight, which detects and can block data exfiltration activities over DNS.
- Frequently patch software; Glupteba propagates by exploiting vulnerable Microsoft Windows Server Message Block (SMB) hosts via EternalBlue.
- Use strong antivirus software and web filtering tools to combat drive-by download attacks.
- Only download software and applications from trusted sources.
- Devices infected by rootkit frequently send TCP/IP packets. Examine unusual patterns or volume of outbound connections in your firewall logs.

Endnotes

1. https://www.infoblox.com/products/threat-insight/
2. https://www.infoblox.com/glossary/dns-tunneling/
3. https://labs.bitdefender.com/2019/12/revisiting-glupteba-still-relevant-five-years-after-debut/
4. https://news.sophos.com/en-us/2020/06/24/glupteba-report/
5. https://twitter.com/James_inthe_box/status/1293305070491074560

Infoblox Cyber Intelligence Unit

With 10 years of experience, the Infoblox Cyber Intelligence Unit creates, aggregates and curates information on threats to provide actionable intelligence that is high-quality, timely and reliable. Threat information from Infoblox minimizes false positives, so you can be confident in what you are blocking, while ensuring a unified security policy across the entire security infrastructure.

Infoblox Threat Intelligence

Infoblox Threat Intelligence enables threat protection using timely and accurate data to minimize organizational risk and protect against cyberattacks. Our data is curated from more than two dozen partners, and our key sources include leading threat intelligence providers, government agencies, universities, as well as the Department of Homeland Security's Automated Indicator Sharing program. Infoblox Threat Intelligence provides a single platform for managing and distributing all of our licensed data sets within an organization's ecosystem.

Infoblox

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud net-working today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70% of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com